BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

EP 000219880 A2
APR 1987

TOKE ★ T01 T05 87-117588/17 ★EP -219-880-A

Data processing terminal device for automatic teller machine - is on/line connected to host computer and records journal data as result of communication on journal paper

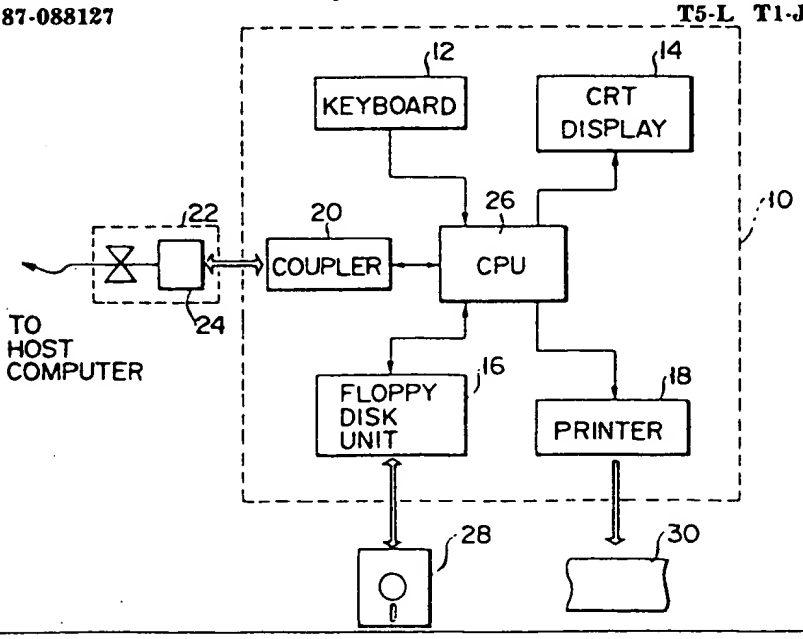
TOSHIBA KK 00.00.86-EP-114801 (09.02.84-JP-022171)
(29.04.87) G07f-07/10
00.00.86 as 114801 (+9.2.84-JP-022172) Related to -151491, filed 7.2.85
(1815SB) (E) No-SR.Pub E(DE FR GB)

The data processing terminal has a unit for recording journal data of communication with the host computer. A converter processes the journal data in accordance with a processing algorithm unknown to a user of the terminal device and converts the journal data to modified data. A device records the modified data, which comprises encrypted journal data used in communication with the host computer.

An encryption key is used for encrypting data. The journal data and the encrypted journal data are printed on journal paper and the encryption key is stored in a programmable read-only memory. The PROM is arranged in a portable device separate from the main terminal unit.

ADVANTAGE - Prevents journal alteration. (27pp Dwg.No.2/13)

N87-088127 T5-L T1-J5A



395-243

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 219 880
A2

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: 86114801.3

(51) Int. Cl.⁴: G 07 F 7/10

(22) Date of filing: 07.02.85

(30) Priority: 09.02.84 JP 22171/84
09.02.84 JP 22172/84
09.02.84 JP 22173/84

(43) Date of publication of application:
29.04.87 Bulletin 87/18

(84) Designated Contracting States:
DE FR GB

(60) Publication number of the earlier application in accordance with Art. 76 EPC: 0 151 491

(71) Applicant: Kabushiki Kaisha Toshiba
72, Horikawa-cho Saiwai-ku
Kawasaki-shi Kanagawa-ken 210(JP)

(72) Inventor: Tamada, Masuo Patent Division K.K. Toshiba
1-1 Shibaura 1-chome Minato-ku
Tokyo 105(JP)

(72) Inventor: Kokuryo, Hitoshi Patent Division K.K. Toshiba
1-1 Shibaura 1-chome Minato-ku
Tokyo 105(JP)

(72) Inventor: Tamura, Shinsuke Patent Division K.K. Toshiba
1-1 Shibaura 1-chome Minato-ku
Tokyo 105(JP)

(72) Inventor: Ozaki, Hiroshi Patent Division K.K. Toshiba
1-1 Shibaura 1-chome Minato-ku
Tokyo 105(JP)

(74) Representative: Henkel, Feiler, Hänzel & Partner
Möhlstrasse 37
D-8000 München 80(DE)

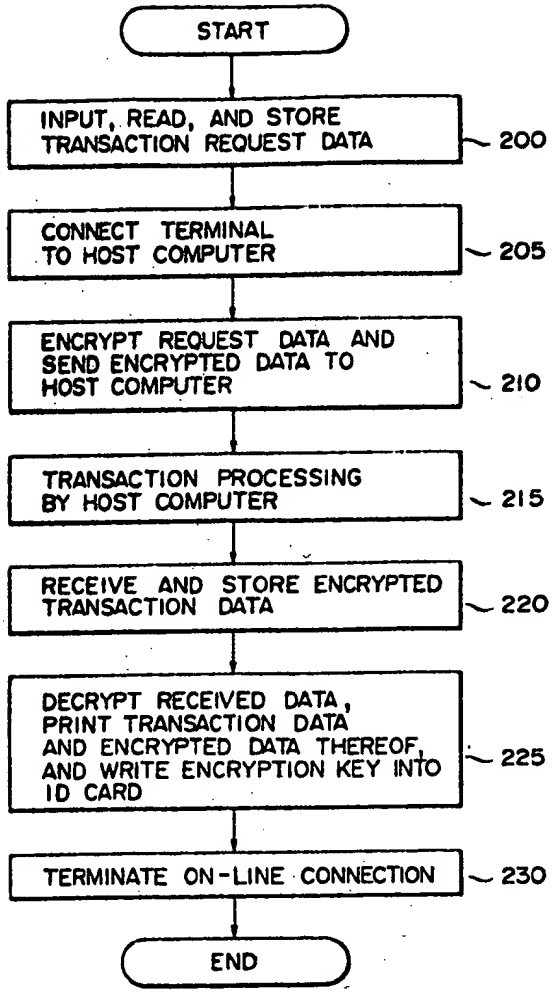
(54) **Data processing terminal device.**

(57) A data processing terminal device is on-line connected to a host computer and records on journal paper journal data obtained as a result of communication with the host computer. Data is encrypted, and encrypted data is exchanged between the terminal device and the host computer. The encrypted journal data is printed together with the normal journal data on the journal paper. By comparing the journal data with its encrypted data, journal data alteration can be easily detected. Additionally, the encrypted data are recorded on an IC card.

EP 0 219 880 A2

./...

FIG. 7


START
INPUT, READ, AND STORE TRANSACTION REQUEST DATA
200
CONNECT TERMINAL TO HOST COMPUTER
205
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
210
TRANSACTION PROCESSING BY HOST COMPUTER
215
RECEIVE AND STORE ENCRYPTED TRANSACTION DATA
220
DECRYPT RECEIVED DATA, PRINT TRANSACTION DATA AND ENCRYPTED DATA THEREOF, AND WRITE ENCRYPTION KEY INTO ID CARD
225
TERMINATE ON-LINE CONNECTION
230
END

Data processing terminal device

The present invention relates to a data processing terminal device (e.g., an automatic teller machine in a bank) which is on-line connected to a host computer and records a journal (result) of communication with the host computer.

Conventional banking terminals such as ATMs (automatic teller machines) are usually installed only in bank branches. However, in keeping with the versatility of recent communication networks, these banking terminals are now being installed in general companies and private homes and are on-line connected with the host computer through a communication network, thereby providing a variety of service applications. In a system having data processing terminal devices installed in locations where banks cannot directly provide maintenance, the following drawback occurs:

In general, the journal representing the transactions is recorded in both the host computer and the terminal device. This recording is performed so that all transactions are printed on journal paper or stored in a floppy disk. The journal recorded in the terminal device is not under the control of the bank and can be altered by a user. For example, a user may bring a journal slip with altered transaction data to a bank and claim he did not perform a particular transaction.

This situation can arise because the journal is recorded in a r writabl recording m dium. A recording medium which cannot be subjected to rewriting at a terminal device is exemplified only by a PROM. In the foregoing circumstance, a PROM having a large memory capacity would be required to store all journal data. Such a PROM cannot be used for this purpose due to high cost.

It is an object of the present invention to prevent journal alteration at a data processing terminal device which is on-line connected to a host computer and which records a journal of communication with the host computer.

In order to achieve the above object the present invention provides a data processing terminal device on-line connected to a host computer, comprising means for recording journal data of communication with said host computer, said data processing terminal device being characterized by further comprising converting means for processing the journal data in accordance with a processing algorithm unknown to a user of the terminal device and converting the journal data to modified data, and means for recording the modified data, wherein the modified data comprises encrypted journal data used in communication with said host computer, and an encryption key used for encrypting data.

A data processing terminal device comprises means for performing processing of journal data which is unknown to a user of the data processing terminal in order to convert the journal data to modified journal data, the journal data and/or the modified journal data being recorded in the data processing device.

This invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a perspective view of a data processing terminal device;

Fig. 2 is a block diagram of the terminal device shown in Fig. 1;

Fig. 3 is a flow chart for explaining the operation of the terminal device shown in Fig. 1;

Fig. 4 is a flow chart for explaining journal data alteration detection in the terminal device of Fig. 1;

Fig. 5 is a perspective view of a data processing terminal device according to an embodiment of the invention;

Fig. 6 is a block diagram of the terminal device shown in Fig. 5;

Fig. 7 is a flow chart for explaining the operation of the terminal device shown in Fig. 5;

Fig. 8 is a flow chart for explaining journal data alteration detection in the terminal device of Fig. 5;

Fig. 9 is a flow chart for explaining data processing in a first modification;

Fig. 10 is a flow chart for explaining journal data alteration detection according to the first modification;

Fig. 11 is a flow chart for explaining data processing according to a second modification;

Fig. 12 is a flow chart for explaining data processing according to a third modification; and

Fig. 13 is a flow chart for explaining journal data alteration detection according to the third modification.

Data processing terminal devices according to the preferred embodiments will be described with reference to the accompanying drawings. Fig. 1 is a perspective view of a data processing terminal device, and Fig. 2 is a block diagram thereof. A terminal device 10 has the same outer appearance as a general personal computer. The terminal device 10 comprises a keyboard 12, a CRT display 14, a floppy disk unit 16, a printer 18, a coupler 20 and a CPU 26 connected to the above components so as to control them. The terminal device 10 is to be installed as an ATM of a bank in a company or private home, but not in a bank branch. The user enters a password and a transaction amount at the keyboard 12. The CRT display 14 displays instruction prompts for causing the user to perform proper operations, and a journal check result to be described later. The floppy disk unit 16 reads out a control program for the CPU 26 from a floppy disk 28 and temporarily stores communication data in the floppy disk

28 when the terminal device 10 communicates with the host computer. The printer 18 prints journal data of transactions on journal paper 30. The coupler 20 is coupled to a handset 24 of a telephone set 22 to convert an electrical signal to an acoustic signal and vice versa so as to on-line connect the CPU 26 to a host computer (not shown).

The operation of the data processing terminal device will be described with reference to a flow chart of Fig. 3. A case will be exemplified wherein a user performs a transfer transaction from his own account to another account and journal data comprises transaction data sent from the host computer which represents the outstanding balance of the user's account after the transfer transaction is completed. When the user depresses a transfer transaction request key at the keyboard 12, the CRT display 14 displays a prompt for transfer transaction request data. The user then enters transaction request data such as a password, a transferee account number, a transfer amount and the like at the keyboard 12. The CPU 26 stores the input transaction request data in the floppy disk 28 (step 100). The CRT display 14 displays a prompt for on-line connection with the host computer in the bank. The user dials the telephone number for the host computer using the telephone set 22 in accordance with this prompt. When the user checks that the connection is made, he couples the handset 24 to the coupler 20, thereby on-line connecting the terminal device 10 to the host computer (step 105). The CPU 26 reads out the transaction request data from the floppy disk 28 in step 110. The readout data is encrypted, and the encrypted data is sent to the host computer. In step 115, the host computer decrypts the encrypted transaction request data and checks the transaction conditions such as the outstanding balance of the transferer's account. When

the transaction conditions satisfy the transaction request data, the outstanding balances of the transferer's and transferee's accounts are adjusted, i.e., updating of the corresponding general ledger is performed. The host computer creates transaction data representing the updated ledger data. The transaction data is encrypted and sent to the terminal device. In step 120, the CPU 26 stores the received encrypted transaction data in the floppy disk 28. In step 125, the CPU 26 reads out the encrypted transaction data from the floppy disk 28 and causes the printer 18 to print the encrypted data and the decrypted transaction data on the journal paper 30. When the user checks an end of communication with the host computer, he removes the handset 24 from the coupler 20 to terminate the on-line connection, as shown in step 130.

The transaction data (journal data) representing the result of the transaction performed by the banking terminal installed in the company or private home is printed together with the corresponding encrypted data on the journal paper 30. In this case, since the encryption algorithm is unknown to the user, alteration of the transaction data in correspondence with its encrypted data cannot be performed excluding an accidental correspondence.

A journal data alteration can be detected by the terminal device in the following journal check mode:

The journal check mode will be described with reference to a flow chart of Fig. 4. In step 150, the terminal device is set in the journal check mode. In step 155, the transaction data and corresponding encrypted data which are printed on the journal paper 30 are entered from the keyboard 12. In step 160, the CPU 26 decrypts the encrypted transaction data in step 160 by using the same algorithm as in step 125 and compares the input transaction data and the decrypted data. If

these data do not coincide with each other, the transaction data and/or its encrypted data which are printed on the journal paper 30 are altered. Coincidence between the transaction data and its encrypted data indicates that no alteration has been performed excluding the case of accidental alteration coincidence. In step 165, the result of the comparison is displayed on the CRT display 14 to indicate whether the journal data has been altered.

As described above, since the journal data and its encrypted data are printed on the journal paper, journal data alteration can be detected by comparing these data.

The journal data and its encrypted data are printed on the journal paper but they can be stored in the floppy disk 28. When the transaction request data is recorded as journal data, it is recorded when it is sent from the terminal device to the host computer. Further, both transaction request data and transaction data may be recorded as journal data. The transaction is not limited to a transfer transaction, but can be extended to a deposit or withdrawal transaction.

An embodiment of the present invention will be described hereinafter. In the above terminal device, the user can perform a transaction when he enters his own account number and the corresponding password. According to this key input operation, however, the user cannot be checked as having the corresponding account. In other words, a third party can use this account. In the present embodiment and subsequent modifications, an ID card which records an account number is issued to an account owner to check whether the rightful user is using the account. No transaction can be performed without using the ID card. The ID card comprises a magnetic card or an IC card.

Fig. 5 is a perspective view of a data processing

terminal device according to the present embodiment, and Fig. 6 is a block diagram thereof. The present embodiment is substantially the same as the above terminal device, except that an ID card reader/writer 40 is included under a floppy disk 16. A card insertion port is formed on the front surface of the ID card reader/writer 40 to receive the ID card 42. Other arrangements of the second embodiment are the same as those of the first embodiment. According to the present embodiment, the ID card 42 is an IC card which has a CPU, a RAM, a ROM and a PROM as a recording medium not subject to data rewriting.

A transaction operation of the present embodiment will be described with reference to a flow chart of Fig. 7. When the user requests a transaction, a prompt is displayed on a CRT display 14 to cause the user to insert his ID card 42 in the ID card reader/writer 40. The user inserts the ID card 42 in the ID card reader/writer 40 through its insertion port. A CPU 26 reads out an account number from the ROM of the ID card 42 and stores the readout data in a floppy disk 28. The CPU 26 causes the CRT display 14 to display prompts requesting transferee's account number and transfer amount data inputs. The user enters the transferee's account number and the transfer amount at a keyboard 12. The CPU 26 enters the input transferee's account number and transfer amount in the floppy disk 28 (step 200). The only difference between steps 100 and 200 is that the account number is entered at the keyboard 12 in step 100, but read out from the ID card 42 in step 200. However, since the ID card 42 is in the possession of the rightful owner, data access safety is improved when the data is read out from the ID card 42. The operations in steps 205 to 220 are the same as those in steps 105 to 120 wherein the host computer performs transaction operations in accordance with the transaction request data and the encrypted transaction

data is sent back to the terminal device and is stored in the floppy disk 28. In the above terminal device, the encryption key is predetermined. However, when the number of journal data is increased, the encryption key might be deduced in accordance with a combination of the transaction data and its encrypted data. In order to prevent this, the encryption key is changed at every transaction or at appropriate intervals in the present embodiment. In step 225, in the same manner as in step 125, the encrypted transaction data is read out from the floppy disk 28, and the readout encrypted transaction data is printed by the printer 18 together with the decrypted transaction data thereof on journal paper 30. The encryption key of the encrypted data read out from the floppy disk 28 is written in the PROM of the IC card 42 in correspondence with the encrypted transaction data. Thereafter, the on-line connection is terminated in step 230.

According to the present embodiment, the transaction data and its encrypted data are printed on the journal paper 30 in the same manner as in above terminal device. In addition, the encryption key changes at every transaction or after appropriate intervals to disable interpretation of the encryption key. As a result, journal data alteration is more difficult.

The journal check mode according to the present embodiment will be described in a flow chart of Fig. 8. The check mode is substantially the same as that of the above terminal device, except that, in step 260, the ID card 42 is inserted in the ID card reader/writer 40 before the encrypted transaction data is decrypted to read out the encryption key corresponding to the encrypted data from the ID card 42, and decryption is performed in accordance with the encryption key.

In the present embodiment, the encryption key is written in the ID card 42. However, another arrangement can be utilized since it is only essential to write the

encryption key in the PROM. For example, the PROM may be arranged in the terminal device, and the encryption key can be written in this PROM or the PROM may be arranged in a portable device other than the ID card. In the present embodiment, data encryption and decryption are performed in the terminal device. However, these operations can be performed in the IC card. The modification made in the above terminal device can also be applied to the present embodiment.

According to the above terminal device and the present embodiment, the journal data and its encrypted data are recorded in one-to-one correspondence, since these data cannot both be altered in the same manner, though they can be respectively altered. Therefore, journal alteration can be detected when these data are compared. It is not important if the encrypted journal data is not recorded together with the journal data, but it is important to record modified data provided by an unknown manner to the user. For this reason, the following first modification will be described wherein the data recorded together with the journal data is not the encrypted data but the modified journal data obtained by processing the journal data in accordance with a technique unknown to the user. In this sense, the encrypted data is a kind of modified data. The perspective view and the block diagram of the first modification are the same as those of the second embodiment shown in Figs. 5 and 6.

Fig. 9 is a flow chart of data processing according to the first modification. Steps 300 to 320 in Fig. 9 are the same as steps 200 to 220 of the above embodiment, respectively. In step 325, the CPU 26 reads out the encrypted transaction data from the floppy disk 28 and decrypts the transaction data. The decrypted transaction data is printed on the journal paper 30. At the same time, the CPU 26 modifies the transaction data in accordance with a predetermined processing scheme. This processing scheme is an exclusive OR calculation of

all bits of the transaction data, extraction of a predetermined bit of the respective data such as outstanding balance data, or four arithmetic operations of the extracted bit. The CPU 26 writes the modified transaction data in the PROM in the ID card 42. Thereafter, the on-line connection is terminated in step 330. Since the modified data is written in the IC card, it is absolutely unalterable. However, since the modification scheme of the modified data is unknown to the user, the modified data can be printed on the journal paper 30 in the same manner as in the above terminal device and the above embodiment.

Journal data alteration detection according to the first modification will be described with reference to a flow chart of Fig. 10. In step 350, the terminal device is set in the journal check mode. The transaction data printed on the journal paper 30 is entered at the keyboard in step 355. In step 360, the CPU 26 reads out the modified transaction data from the ID card 42 inserted in the ID card reader/writer 40. The CPU 26 then converts the input transaction data to the modified transaction data in the same processing as in step 325 and compares these two data. When they do not coincide with each other, the transaction data is altered. However, when they do coincide with each other, the transaction data is not altered. A comparison result is displayed on the CRT display 14 in step 365 to determine whether or not the journal data is altered.

According to the first modification, since the reference modified transaction data is written in the IC card and cannot be altered, a noncoincidence between the data in the IC card and the data written on the journal paper 30 represents an alteration of the transaction data written on the journal paper 30. The modification made in the above terminal device can also be applied to the present first modification.

Fig. 11 is a flow chart for explaining data

processing according to a second modification. The second modification is substantially the same as the first modification, except that decryption of encrypted transaction data read out from the floppy disk 28 and conversion of the readout transaction data to modified transaction data are not performed in the terminal device but in the IC card, as shown in steps 420 and 425. The journal data alteration detection according to the second modification is the same as that of Fig. 10, and a description thereof will be omitted.

In the first and second modifications, the encrypted transaction data read out from the floppy disk 28 is decrypted, and the decrypted transaction data is processed in accordance with the predetermined modification scheme, thereby obtaining the modified encrypted transaction data. However, the encrypted transaction data read out from the floppy disk 28 may be directly processed to obtain modified encrypted transaction data. In this case, in the journal check mode, the transaction data entered at the keyboard is encrypted and processed in accordance with the predetermined modification scheme, thereby obtaining the modified encrypted transaction data.

In the terminal devices, embodiments and modifications described above, only one reference data for a comparison excluding the journal data is recorded, and journal data alteration is detected by a single comparison operation. However, a plurality of combinations of reference data may be recorded to check for any alterations of the journal data in accordance with a plurality of comparison operations as exemplified by a third modification.

Fig. 12 is a flow chart for explaining data processing according to the third modification. Steps 500 to 515 of the third modification are the same as steps 400 to 415 of the second modification, respectively. In step 520, the CPU 26 reads out the encrypted transaction data from the floppy disk 28. The readout data is processed

in accordance with the predetermined modification scheme to obtain modified encrypted transaction data. The modified encrypted transaction data is written in the IC card 42. In step 525, the CPU 26 decrypts the encrypted transaction data read out from the floppy disk 28 and prints the decrypted transaction data and the transaction data together on the journal paper 30. Thereafter, in step 530, the on-line connection is terminated. In this manner, according to the third modification, the journal data is printed together with the encrypted data on the journal paper 30. At the same time, the modified data of the encrypted journal data is written in the IC card.

The journal check mode according to the third modification will be described with reference to a flow chart of Fig. 13. In step 550, the terminal device is set in the journal check mode. In step 555, the transaction data and its encrypted data which are printed on the journal paper 30 are entered. In step 560, the CPU 26 decrypts the encrypted transaction data in accordance with the same algorithm as in step 525. The CPU 26 compares the decrypted data with the input transaction data. At the same time, the CPU 26 reads out the modified encrypted transaction data from the IC card 42 inserted in the ID card reader/writer 40 and converts the key input encrypted transaction data to modified encrypted transaction data in the same modification scheme as in step 520. The CPU 26 then compares these two modified transaction data. When a noncoincidence is detected by the CPU 26, the CPU 26 detects that the transaction data and/or its encrypted data which is written on the journal paper 30 is altered. When a coincidence is detected by the CPU 26, the CPU 26 detects that the transaction data and its encrypted data have not been altered. According to the third modification, double checking is performed to improve detection precision of data alteration.

According to the present invention, as described in detail, the modified journal data which is processed in accordance with a manner unknown to the user is recorded together with the normal journal data. When the journal data is compared with the corresponding modified data, journal data alteration can be easily detected.

The present invention is not limited to the particular embodiments described above. Various changes and modifications can be made within the spirit and scope of the invention.

Claims:

1. A data processing terminal device on-line connected to a host computer, comprising:

means for recording journal data of communication with said host computer;

characterized by further comprising

converting means for processing the journal data in accordance with a processing algorithm unknown to a user of the terminal device and converting the journal data to modified data; and

means for recording the modified data,

wherein the modified data comprises encrypted journal data used in communication with said host computer, and an encryption key used for encrypting data.

2. A device according to claim 1, characterized in that the journal data and the encrypted journal data are printed on journal paper, and the encryption key is stored in a programmable read-only memory.

3. A device according to claim 2, characterized in that said programmable read-only memory is arranged in a portable device provided separately from the main unit of said data processing terminal device, the portable device being issued to the user.

FIG. 1

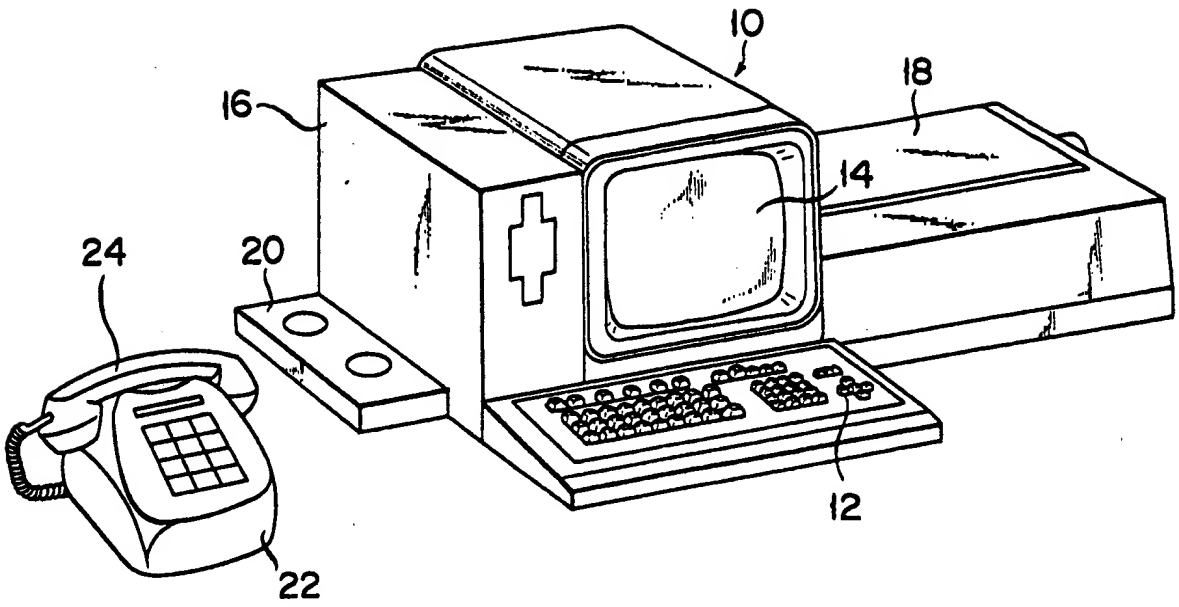

10
16
18
14
24
20
12
22

FIG. 2

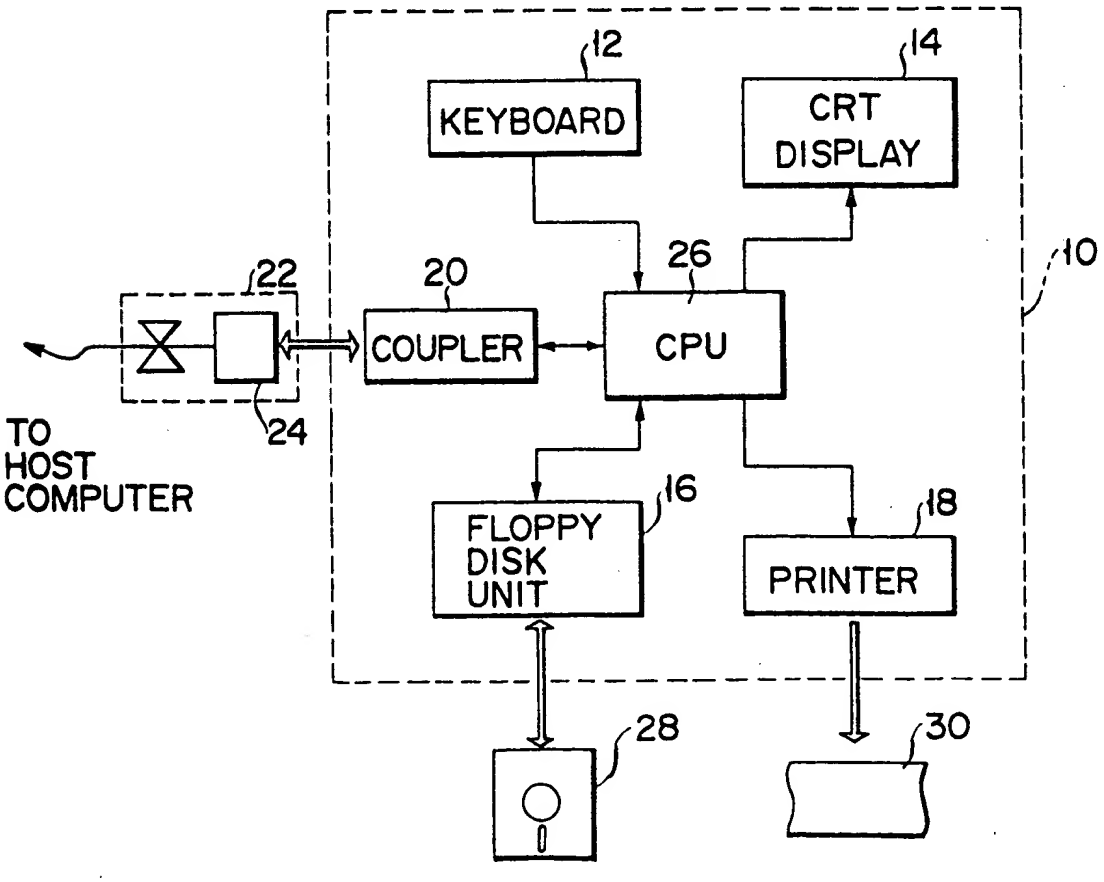

12
KEYBOARD
14
CRT DISPLAY
26
10
22
20
COUPLER
CPU
24
TO HOST COMPUTER
16
FLOPPY DISK UNIT
18
PRINTER
28
30

FIG. 3

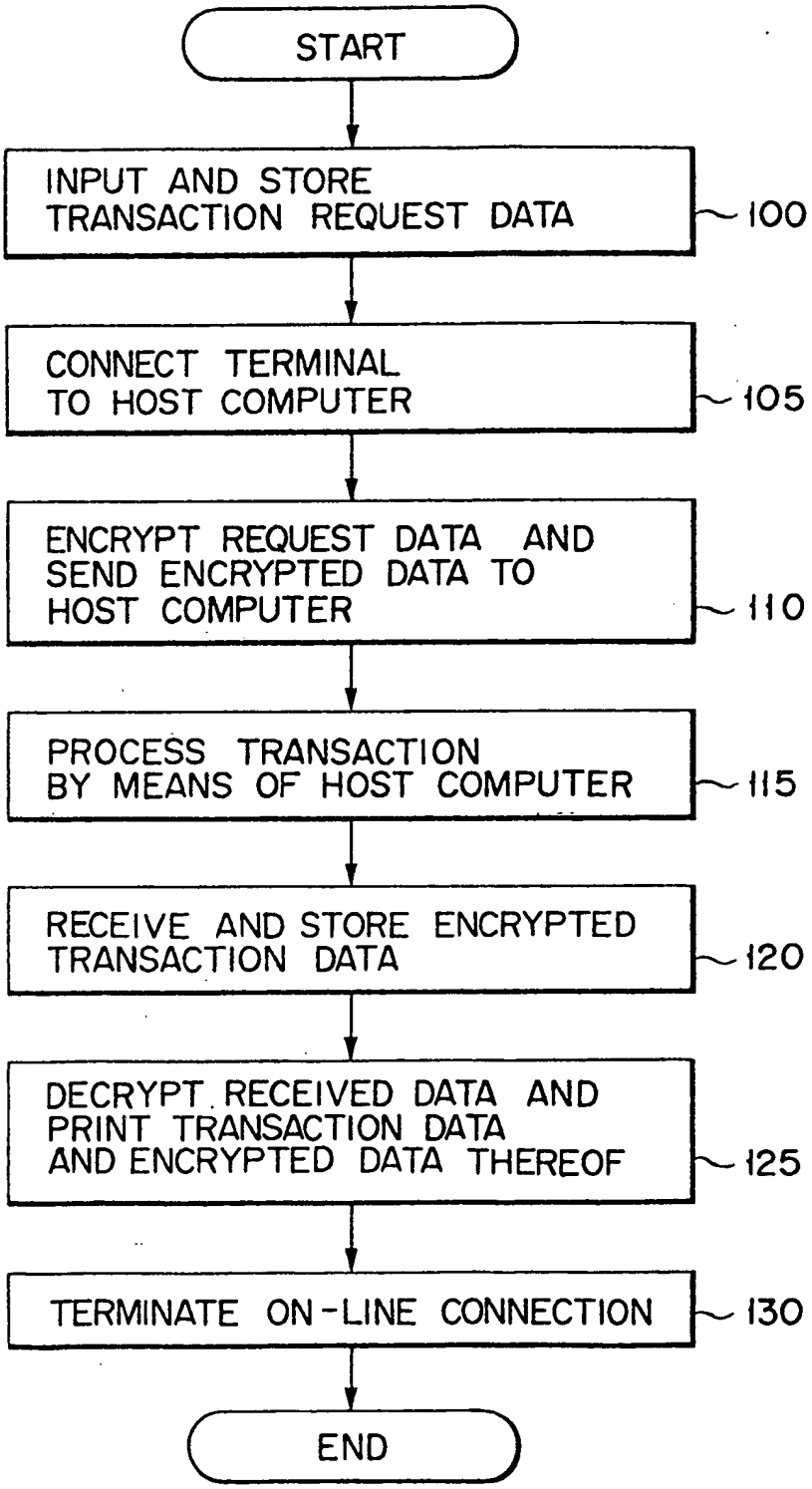

START
INPUT AND STORE TRANSACTION REQUEST DATA
100
CONNECT TERMINAL TO HOST COMPUTER
105
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
110
PROCESS TRANSACTION BY MEANS OF HOST COMPUTER
115
RECEIVE AND STORE ENCRYPTED TRANSACTION DATA
120
DECRYPT RECEIVED DATA AND PRINT TRANSACTION DATA AND ENCRYPTED DATA THEREOF
125
TERMINATE ON-LINE CONNECTION
130
END

FIG. 4

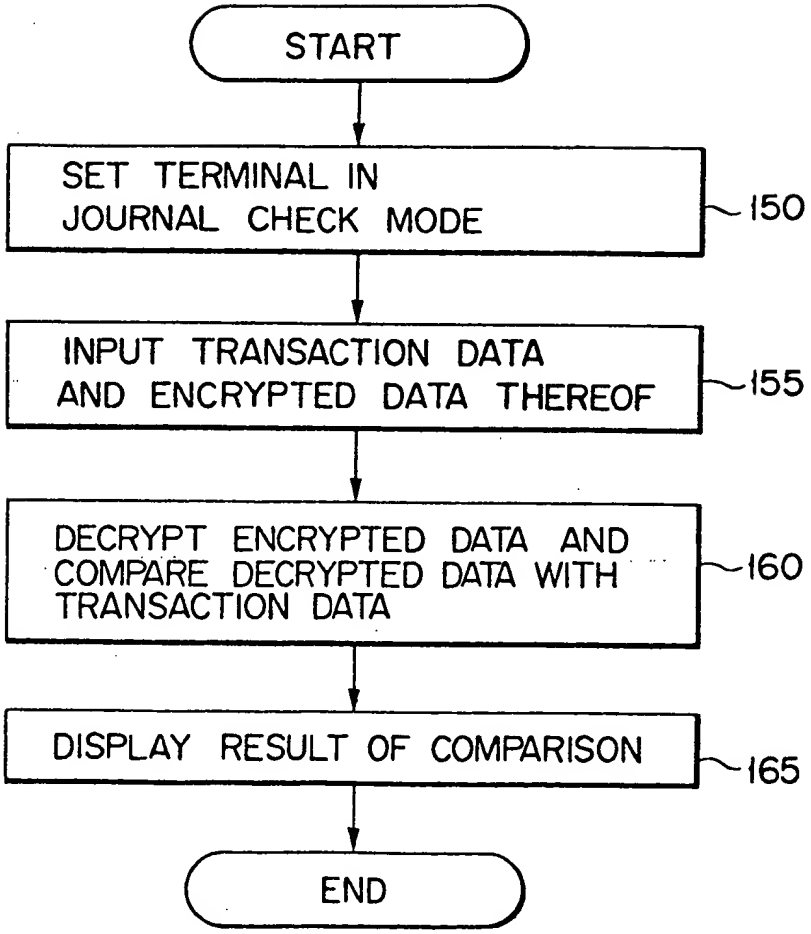

START
SET TERMINAL IN JOURNAL CHECK MODE
150
INPUT TRANSACTION DATA AND ENCRYPTED DATA THEREOF
155
DECRYPT ENCRYPTED DATA AND COMPARE DECRYPTED DATA WITH TRANSACTION DATA
160
DISPLAY RESULT OF COMPARISON
165
END

FIG. 5

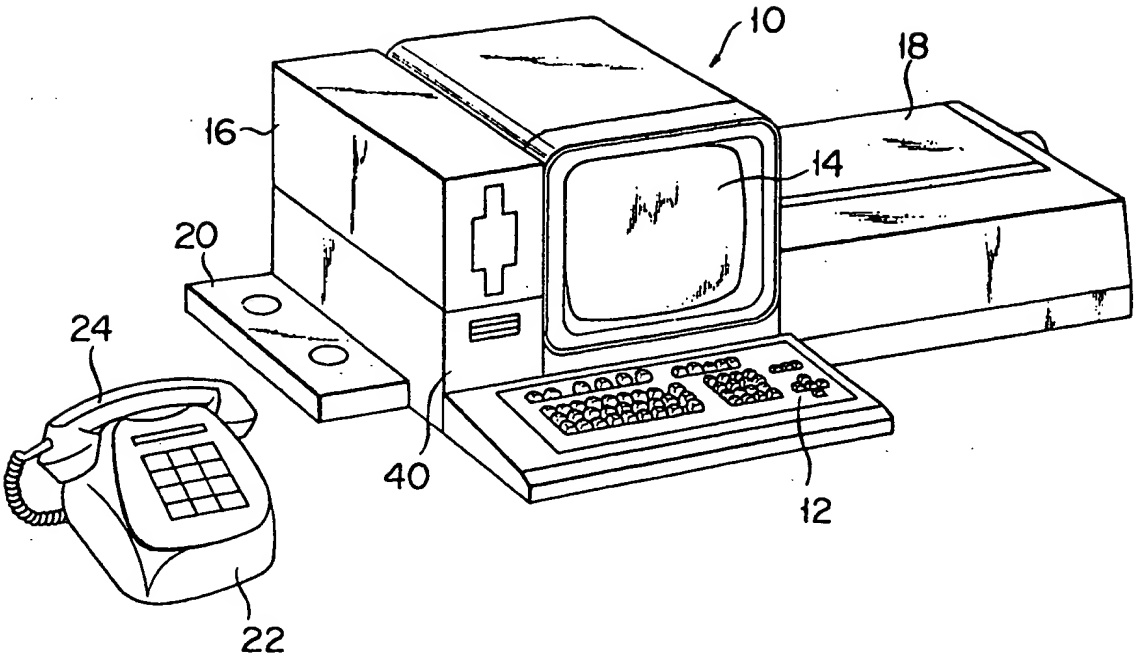

10
18
16
14
20
24
40
12
22

FIG. 6

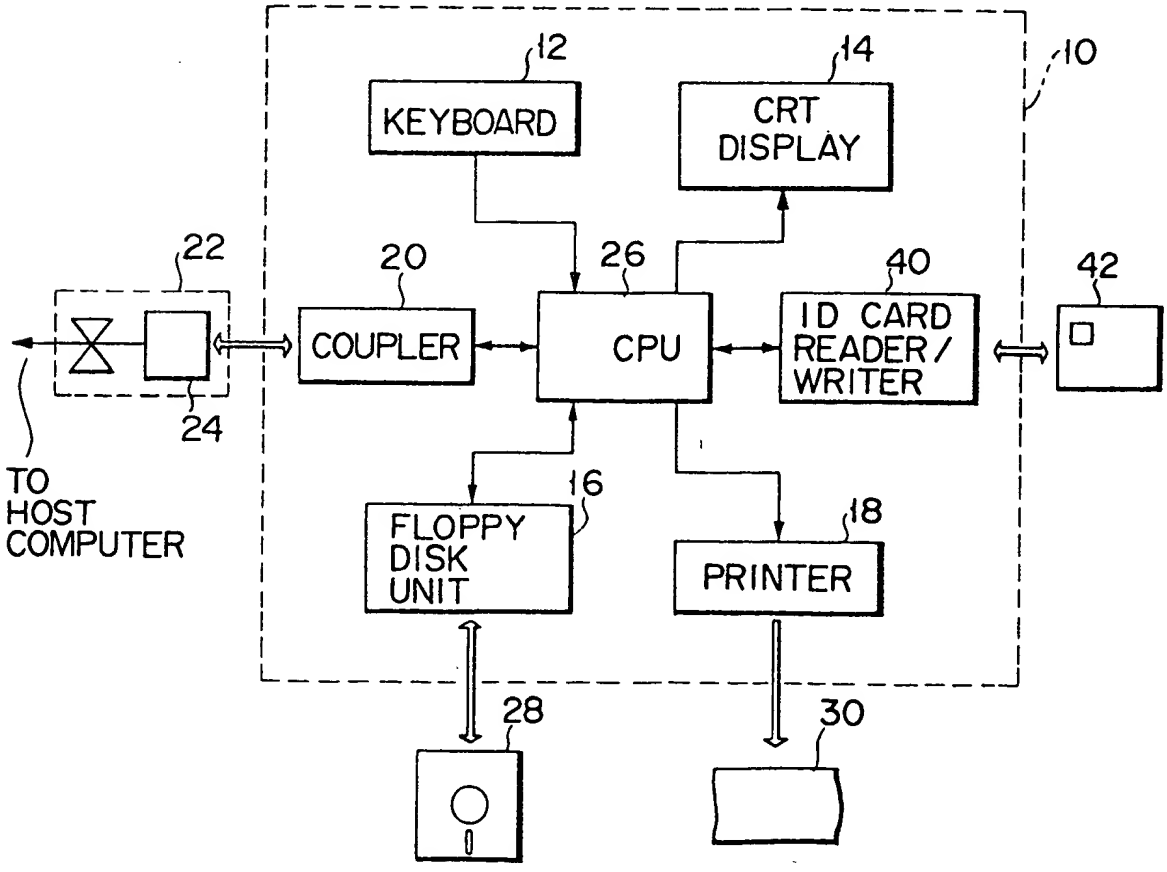

12
KEYBOARD
14
CRT DISPLAY
10
22
20
26
40
42
COUPLER
CPU
ID CARD READER/ WRITER
24
TO HOST COMPUTER
16
FLOPPY DISK UNIT
18
PRINTER
28
30

FIG. 7

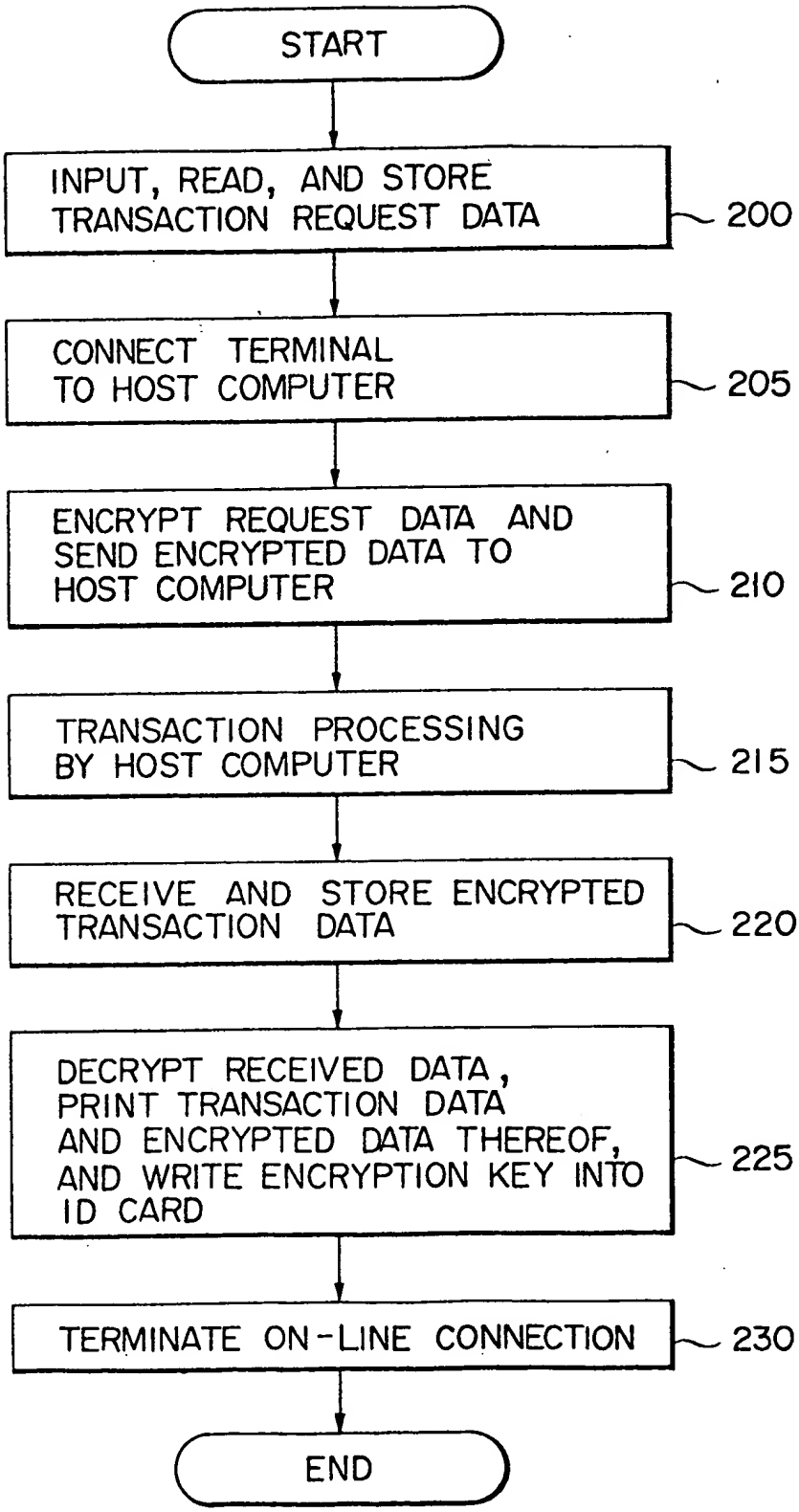

START
INPUT, READ, AND STORE TRANSACTION REQUEST DATA
200
CONNECT TERMINAL TO HOST COMPUTER
205
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
210
TRANSACTION PROCESSING BY HOST COMPUTER
215
RECEIVE AND STORE ENCRYPTED TRANSACTION DATA
220
DECRYPT RECEIVED DATA, PRINT TRANSACTION DATA AND ENCRYPTED DATA THEREOF, AND WRITE ENCRYPTION KEY INTO ID CARD
225
TERMINATE ON-LINE CONNECTION
230
END

FIG. 8

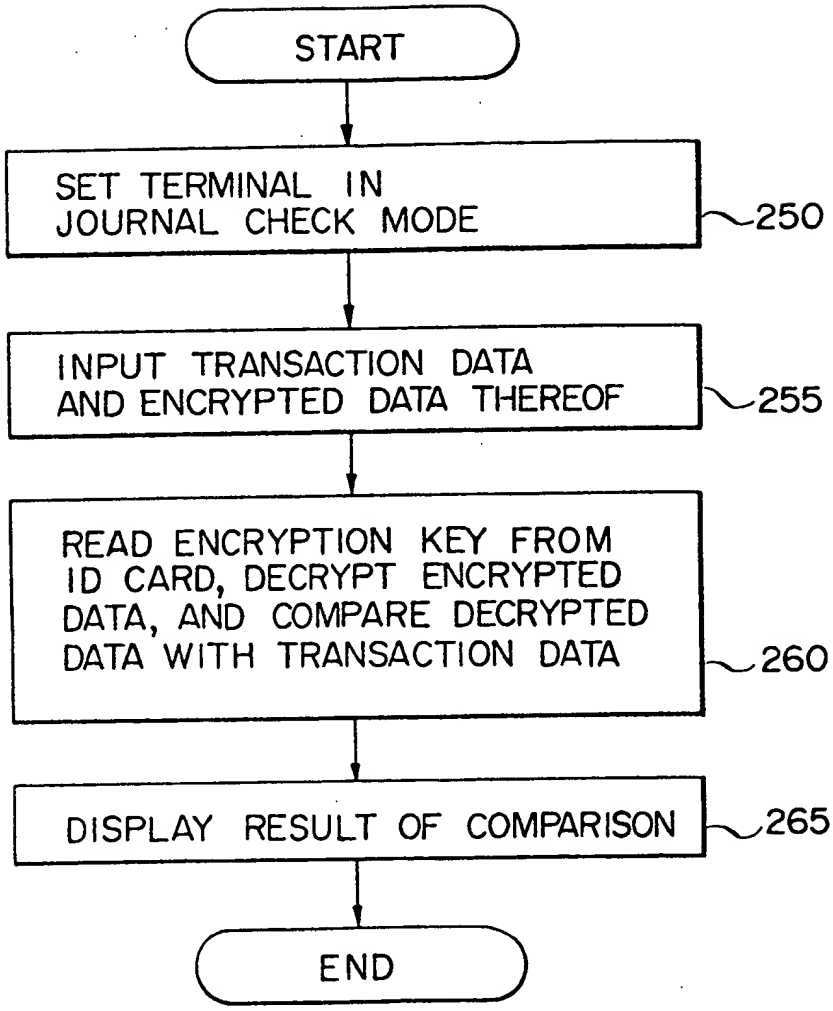

START
SET TERMINAL IN JOURNAL CHECK MODE
250
INPUT TRANSACTION DATA AND ENCRYPTED DATA THEREOF
255
READ ENCRYPTION KEY FROM ID CARD, DECRYPT ENCRYPTED DATA, AND COMPARE DECRYPTED DATA WITH TRANSACTION DATA
260
DISPLAY RESULT OF COMPARISON
265
END

FIG. 9

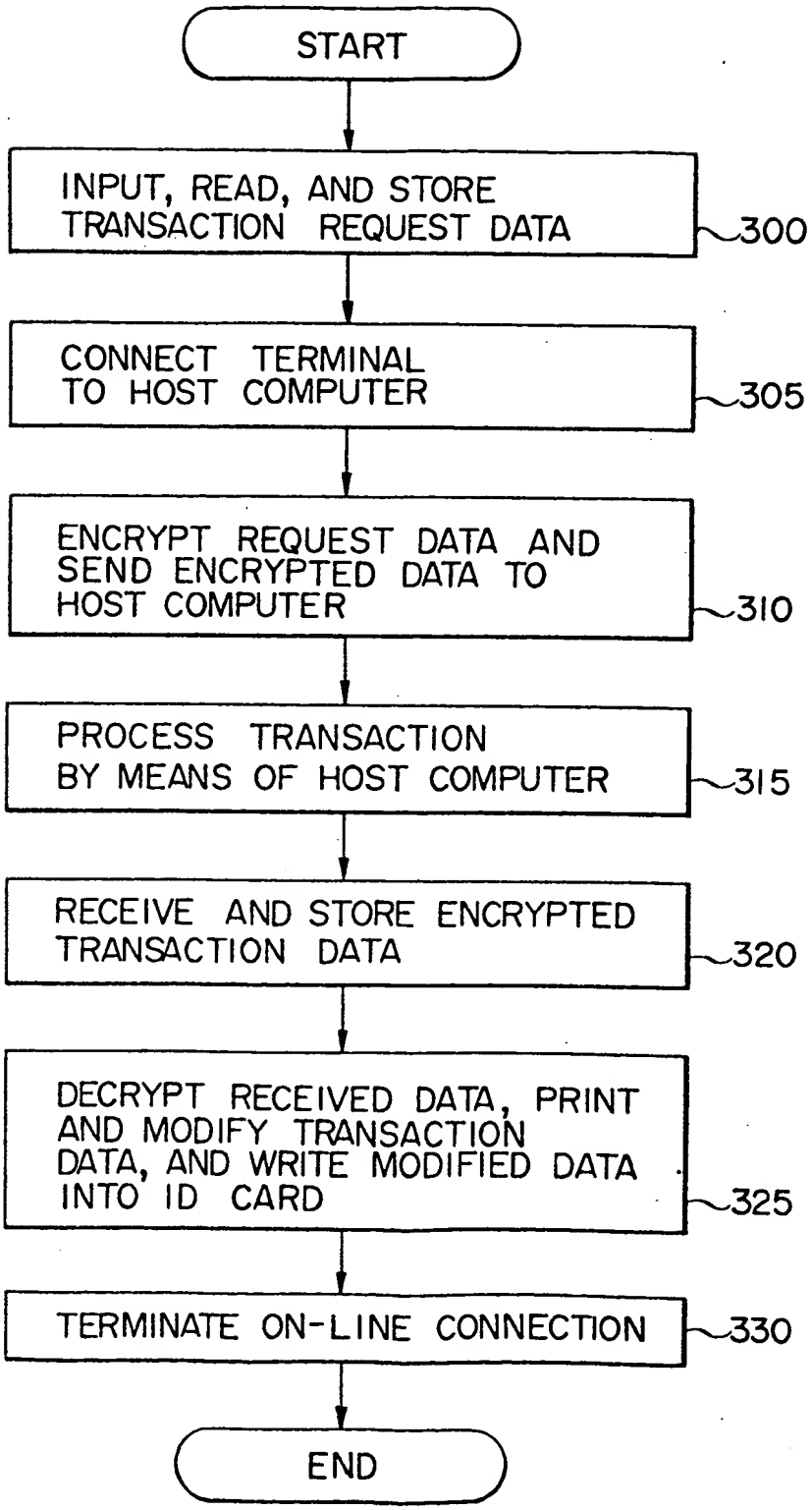

START
INPUT, READ, AND STORE TRANSACTION REQUEST DATA
300
CONNECT TERMINAL TO HOST COMPUTER
305
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
310
PROCESS TRANSACTION BY MEANS OF HOST COMPUTER
315
RECEIVE AND STORE ENCRYPTED TRANSACTION DATA
320
DECRYPT RECEIVED DATA, PRINT AND MODIFY TRANSACTION DATA, AND WRITE MODIFIED DATA INTO ID CARD
325
TERMINATE ON-LINE CONNECTION
330
END

FIG. 10

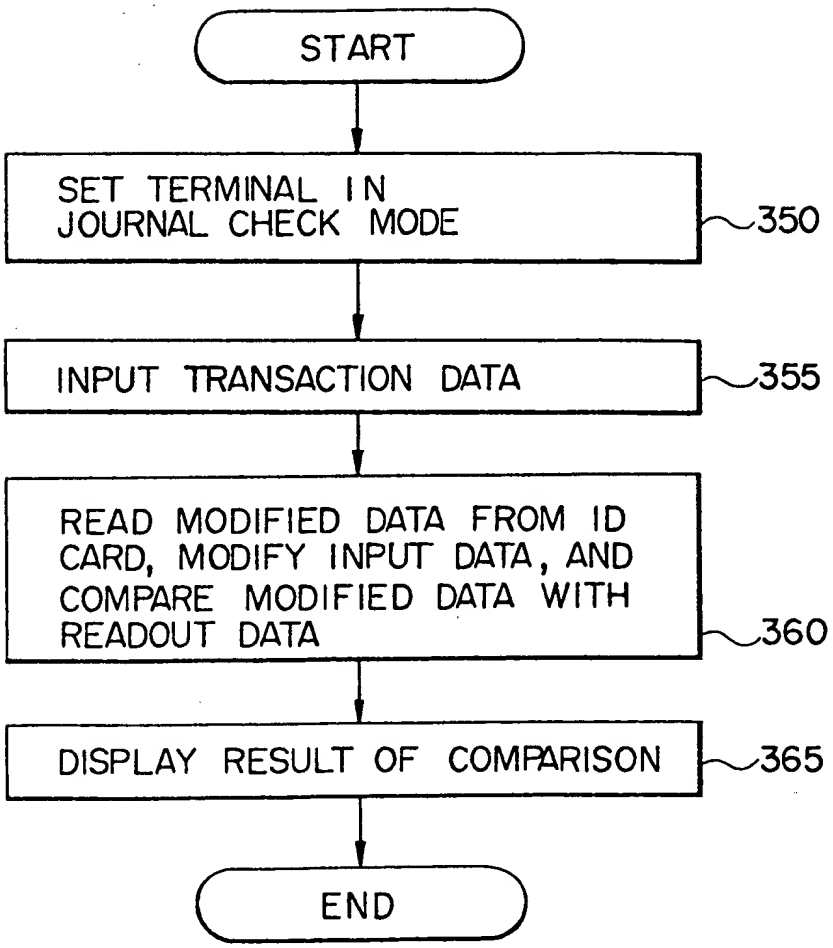

START
SET TERMINAL IN JOURNAL CHECK MODE
350
INPUT TRANSACTION DATA
355
READ MODIFIED DATA FROM ID CARD, MODIFY INPUT DATA, AND COMPARE MODIFIED DATA WITH READOUT DATA
360
DISPLAY RESULT OF COMPARISON
365
END

FIG. 11

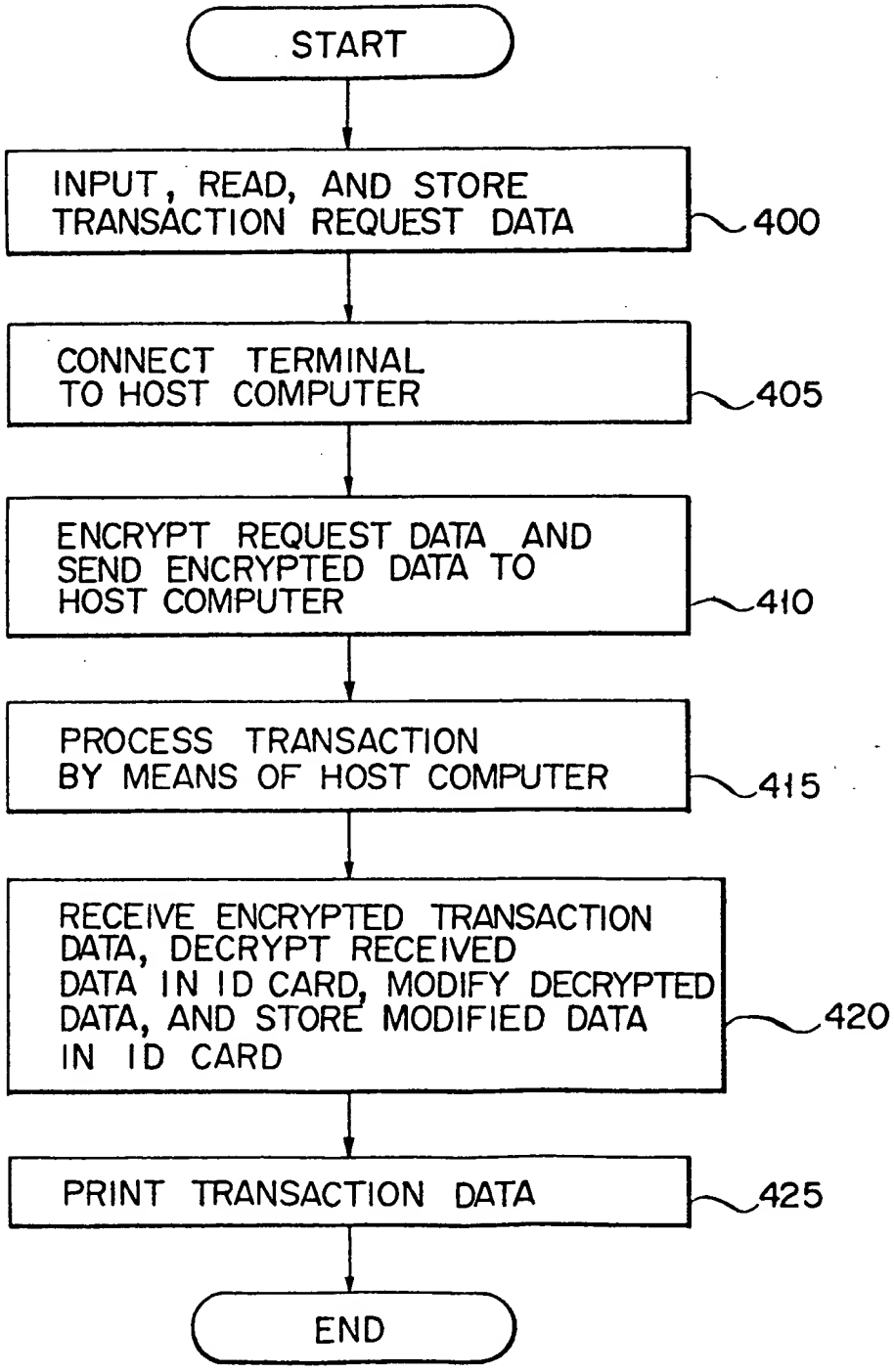

START
INPUT, READ, AND STORE TRANSACTION REQUEST DATA
400
CONNECT TERMINAL TO HOST COMPUTER
405
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
410
PROCESS TRANSACTION BY MEANS OF HOST COMPUTER
415
RECEIVE ENCRYPTED TRANSACTION DATA, DECRYPT RECEIVED DATA IN ID CARD, MODIFY DECRYPTED DATA, AND STORE MODIFIED DATA IN ID CARD
420
PRINT TRANSACTION DATA
425
END

FIG. 12

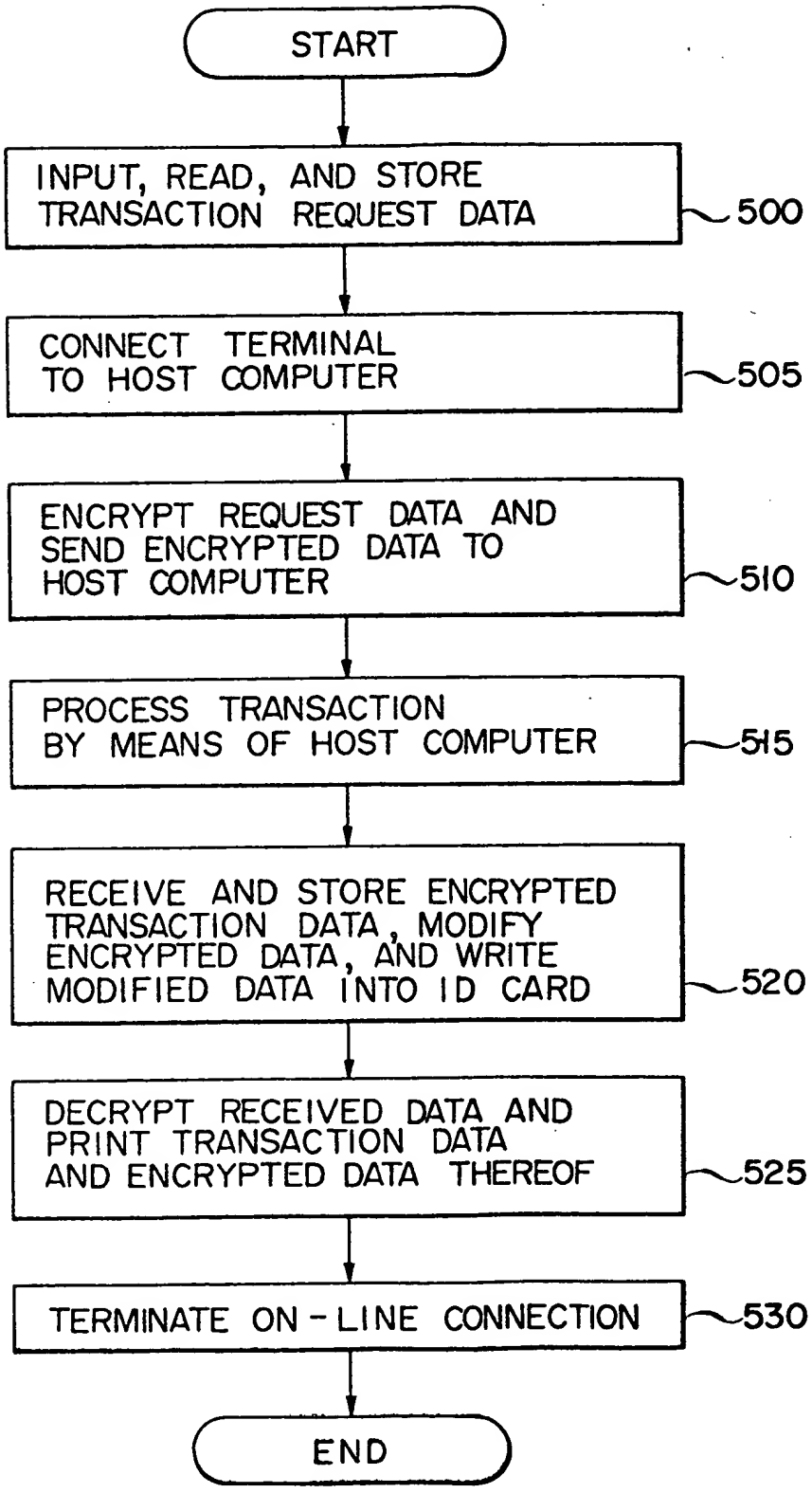
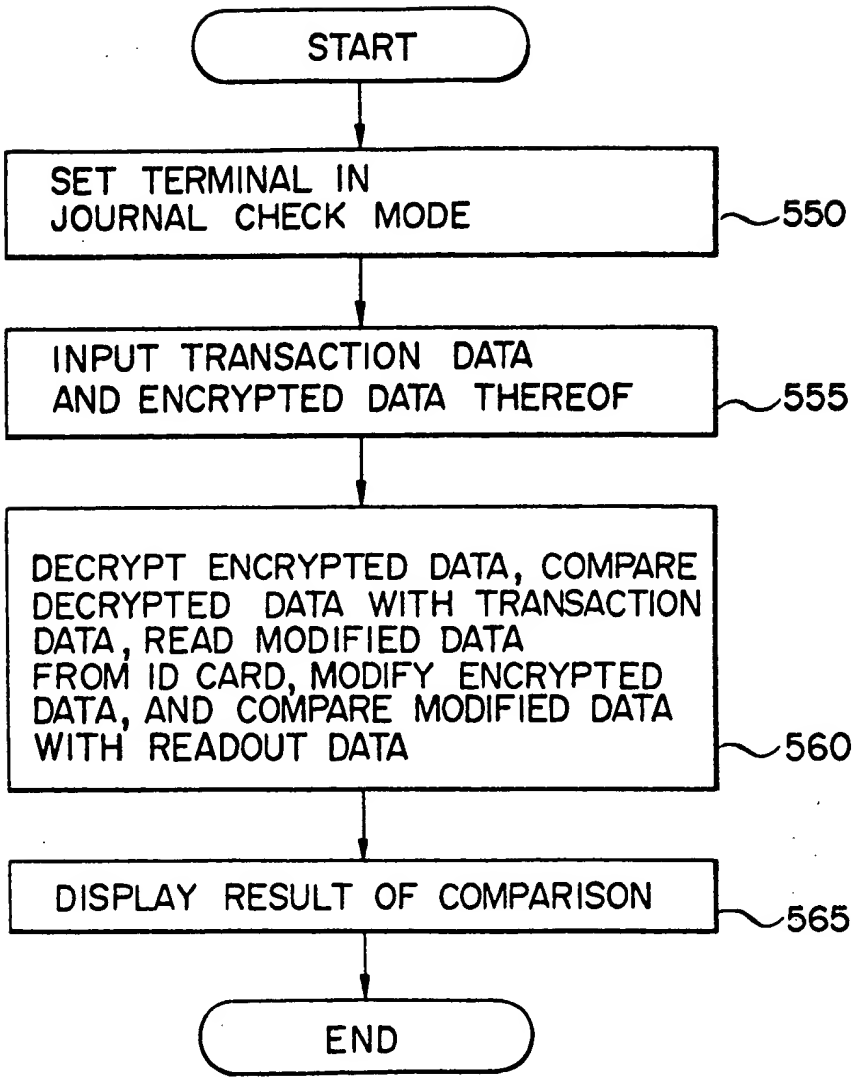

START
INPUT, READ, AND STORE TRANSACTION REQUEST DATA
500
CONNECT TERMINAL TO HOST COMPUTER
505
ENCRYPT REQUEST DATA AND SEND ENCRYPTED DATA TO HOST COMPUTER
510
PROCESS TRANSACTION BY MEANS OF HOST COMPUTER
515
RECEIVE AND STORE ENCRYPTED TRANSACTION DATA, MODIFY ENCRYPTED DATA, AND WRITE MODIFIED DATA INTO ID CARD
520
DECRYPT RECEIVED DATA AND PRINT TRANSACTION DATA AND ENCRYPTED DATA THEREOF
525
TERMINATE ON-LINE CONNECTION
530
END

FIG. 13


START
SET TERMINAL IN JOURNAL CHECK MODE
550
INPUT TRANSACTION DATA AND ENCRYPTED DATA THEREOF
555
DECRYPT ENCRYPTED DATA, COMPARE DECRYPTED DATA WITH TRANSACTION DATA, READ MODIFIED DATA FROM ID CARD, MODIFY ENCRYPTED DATA, AND COMPARE MODIFIED DATA WITH READOUT DATA
560
DISPLAY RESULT OF COMPARISON
565
END